

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DISTRICT

UNITED STATES OF AMERICA,)
)
)
Plaintiff,)
)
v.) No. 4:18CR0876 JAR
)
)
ASHU JOSHI,)
)
Defendant.)

**GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS
EVIDENCE**

Comes now the United States of America, by and through its attorneys, Jeffrey B. Jensen, United States Attorney for the Eastern District of Missouri, and Colleen Lang, Assistant United States Attorney for said district, and files its Response to Defendant's Motions to Suppress Evidence, Doc. #117.

I. INTRODUCTION

Defendant moves to suppress evidence seized in this case on the grounds that the evidence was obtained from an illegal search. Specifically, the defendant moves to suppress his statement, his Facebook messages, his photographs, and his consent to search his residence. The defendant had filed separate motions to suppress the indictment and statements. The Government will only respond to the defendant's motion to suppress the evidence in this response.

The evidence presented within this response and at the hearing will show that the searches were originally performed by a third party and none of the evidence was illegally obtained. Defendant did not have a reasonable expectation of privacy in files that he shared on

Facebook's platform. Facebook notifies users in their terms and conditions that Facebook bans some content. Further, Facebook is not a government agent because it is not required to scan its' network for child pornography, but if it comes across it, it will report criminal activity to law enforcement.

II. FACTUAL BACKGROUND¹

A. Cyber-Tips Reported to Law Enforcement.

On October 9, 2018, Sargent Adam Kavanaugh received from the Bowling Green, Kentucky Police Department, four (4) cyber-tips from the National Center for Missing and Exploited Children (hereafter "NCMEC"). The Bowling Green Police Department was seeking assistance in a case they were investigating involving the aforementioned cyber-tips and a sixteen-year old child by the name of "M.D." The cyber-tips had been forwarded to NCMEC from Facebook. NCMEC received the cyber-tips on October 5 and 6, 2018. The cyber-tips showed that M.D. and an adult male named Ashu Joshi had been exchanging child pornography photographs of M.D. via Facebook messenger. Also in the cyber-tips provided by Facebook, it is evident that Ashu Joshi is requesting M.D. to take photographs of her genitals and send it to him over Facebook messenger².

In total, Facebook had flagged and sent to NCMEC 450 images of child exploitation material from the defendant and the victim's Facebook accounts.

On October 10, 2018, Sgt. Kavanaugh contacted Det. Buss at the Bowling Green Police

¹ The background and factual summary information provided is intended as a general guide to aid the Court. It is not intended as a comprehensive statement of the government's case.

² Facebook Messenger is an application available to Facebook users, which allows them to have written text conversations between two or more people via the Facebook platform.

Department and learned that the Bowling Green Police had positively identified M.D. and Ashu Joshi. Det. Buss told Sgt. Kavanaugh that Ashu Joshi was a forty-seven year old adult male living in St. Louis County, Missouri. The detectives had identified M.D. as a sixteen-year old female student at high school in Bowling Green, but she had been recently pulled out of that school.

B. Defendant's Confession.

On October 10, 2018, FBI Special Agent Nikki Badolato and Detective Andrew Lucca responded to SLU Hospital to locate and interview Ashu Joshi. Ashu Joshi worked at the hospital. SA Badolato and Det. Lucca met the defendant, Ashu Joshi, at the security office. He was transported back to the St. Louis County Police Department Headquarters and placed in an interview room at 12:32 p.m. Det. Lucca began the interview by reading the defendant his *Miranda* rights, defendant stated he understood his rights and was willing to speak with Det. Lucca. Defendant told Det. Lucca that he met M.D. through her mother and knew she was only sixteen-years old. The defendant admitted that M.D. and himself had exchanged "many, many" naked photographs of M.D. over Facebook messenger. The defendant also admitted to taking photographs of M.D. in which she is nude and directing her to take photographs of herself in a lascivious display of her genitals. Defendant admitted he has a Facebook account in his name, Ashu Joshi, and Det. Lucca explained to him why that account is now suspended³. Det. Lucca showed the defendant the images and chats received from Facebook and the defendant admitted those are messages and photographs he exchanged with the minor victim. The defendant

³ The defendant's Facebook account was suspended at the beginning of October of 2018 because the child exploitative material he possessed on the account violated Facebook's terms and conditions. When the account was suspended, the defendant no longer had access to it.

admitted to traveling to Kentucky to meet the victim and also driving the victim back to Missouri on two occasions. The interview remains non-confrontational, casual, and relaxed throughout the whole the interview.

The defendant voluntarily signed multiple consent forms for the police to look at his cell phone, his digital devices, and to search his residence.

C. Victim's Interview.

Also on October 10, 2019, in Bowling Green Kentucky, investigators were attempting to locate the victim. After not locating her in Bowling Green, they realized she had moved back to Corbin, Kentucky. The detectives got in the car and made the three hour drive to Corbin, Kentucky. Once in Corbin, they went to an address for the victim on Sandy Hill. However, the victim and her mother are no longer living at that address. They continued to investigate, checking several different addresses, before finally locating the victim at her new residence late in the evening of October 10, 2019.

The victim, M.D., was interviewed by Sgt. Oliver of the Kentucky State Police. M.D. stated to Sgt. Oliver that Patricia Dole was her mother and legal guardian, but not her biological mother. M.D. stated she is sixteen years old and did not know why the police were at her home. M.D. explained to police that she just moved back to her mother's home in Corbin. She had been living in Bowling Green, Kentucky, with her sister. During this interview, M.D. at first told Sgt. Oliver that Ashu Joshi was just a friend, but later in the questioning, she admits to being in a sexual relationship with the defendant. She does not say they are married or engaged. M.D. stated that she used to babysit for the defendant and knows him through her mother. M.D. stated that she went to St. Louis once to watch the defendant's baby. M.D. stated that her mom only gave them (defendant and herself) permission to talk. At first M.D. stated her and the

defendant had not had sex, but later stated that she is pregnant and it may be his baby. M.D. was told that the defendant's Facebook account was shut down because of the images of child pornography of her on his account. M.D. admitted to sending and receiving the images in question on Facebook with the defendant.

D. Criminal Proceedings.

A criminal complaint was filed against the defendant on October 11, 2019, in federal court, defendant was arrested by federal authorities, and the defendant was brought before Magistrate Judge David D. Noce. On October 24, 2018, a Grand Jury indicted the defendant for the crimes of Production of Child Pornography, Interstate Transportation of a Minor, and Distribution of Child Pornography. Doc. #17.

The government received and served two valid federal search warrants on Facebook for evidence of crimes of child exploitation in this case. The search warrants for were for the Facebook account of the victim and the account of defendant. Facebook complied and returned those results to the FBI. Defendant withdrew his consent for law enforcement to search his cell phone and other computer devices on November 21, 2018. The FBI subsequently received a lawful federal search warrant for those devices.

III. LEGAL ANALYSIS OF EVIDENCE SUPPRESSION ISSUES

A. Defendant Does Not Have a Reasonable Expectation of Privacy When on Facebook.

The defendant alleges that his Fourth Amendment rights were violated by an illegal search of his communications on Facebook. The defendant relies on *Kyllo v. United States*, 533 U.S. 27 (2001) to argue that his reasonable expectation of privacy was violated when Facebook saw his illegal communication and turned it over to authorities. However, *Kyllo* is not a

comparable case in these circumstance. *Kyllo* dealt with the government searching someone's personal space, not a third party, which is what we have in this case. Here, Facebook located and found illicit and illegal material in the defendant's account and notified NCMEC, who in turn, notified law enforcement.

The Fourth Amendment protects individuals against "unreasonable searches and seizures" by the government and protects privacy interests where an individual has a reasonable expectation of privacy. *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). A defendant who is seeking to suppress evidence from a search must demonstrate that he had a "legitimate expectation of privacy" in the place searched. *United States v. Hamilton*, 538 F.3d 162, 167 (2d Cir. 2008). This inquiry involves the court to ask two separate questions. First, the court must determine whether the individual had a subjective expectation of privacy. Second, the court must determine whether that expectation of privacy is one that society accepts as reasonable. *Katz v. United States*, 389 U.S. 347, 361 (1967).

[I]n *United States v. Miller*, 425 U.S. 435 (1976), and *Smith*, 442 U.S. 735 (1979), the Supreme Court developed a bright-line application of the reasonable-expectation-of-privacy test that is relevant here. In what has come to be known as the "third-party doctrine," the Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties ... even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Smith*, 442 U.S. at 743-44 (citing *Miller*, 425 U.S. at 442-44).

In this case, the defendant chose to use the Facebook messenger application to produce, receive and exchange images of child pornography and related messages. By using Facebook, a social media platform, the defendant put his private communications in the hands of a third

party. To become a Facebook user, the defendant had to agree to their terms and conditions. These conditions include not violating Facebook's "Community Standards," and other terms and polices. Facebook does not allow, "content that sexually exploits or endangers children." And in their terms and conditions warns the user that, "we report it to the National Center for Missing and Exploited Children (NCMEC)."⁴ Facebook's terms and conditions also prohibits bullying, some adult nudity, sexual exploitation of adults, images of self-injury, and other communications that are not illegal, but are banned from Facebook. Facebook is not a government entity and the government has no control over what Facebook does and does not regulate.

Secondly, Facebook and its' Facebook messenger application, are free. Facebook does not charge a fee to use the services or the social media application. Common sense should tell any user, that free is not really free, because Facebook, like any other company is trying to make money. Thus, if a user reads the terms and conditions, it is clear that Facebook is collecting your private and personal information to give to advertisers:

Instead of paying to use Facebook and the other products and services we offer, by using the Facebook Products covered by these Terms, you agree that we can show you ads that businesses and organizations pay us to promote on and off the Facebook Company Products. We use your personal data, such as information about your activity and interests, to show you ads that are more relevant to you. . .

We collect and use your personal data in order to provide the services described above to you. You can learn about how we collect and use your data in our Data Policy. You have controls over the types of ads and advertisers you see, and the types of information we use to determine which ads we show you. Learn more.

Facebook's terms and conditions. <https://www.facebook.com/terms.php>

Under Facebook's data policy, they state that, "we collect the content, communications, and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others."

⁴ <https://www.facebook.com/communitystandards/safety>

<https://www.facebook.com/about/privacy/update>. Therefore, there is no reasonable expectation of privacy on any of Facebook's platforms. Facebook clearly tells its' users in their terms of service that they are collecting their personal data, their messages, and then they are sharing it with advertisers. Facebook makes money off the ads and by selling information to advertisers, while use of their products is free. Also, in April of 2018, Mark Zuckerberg was interviewed by a reporter at the publication "Vox," and admitted that the company is monitoring the messages on Facebook messenger and had even stopped and prevented messages on Facebook messenger that could have incited violence.⁵ There is no reasonable expectation of privacy on a social medial application, especially on an application that is free to download, use, and readily acknowledges that it collects and analyzes users' data.

The defendant attempts to rely on *Kyllo v. United States*, 533 U.S. 27 (2001); *United States v. Jones*, 565 U.S. 400 (2012); and *Florida v. Jardines*, 133 S.Ct. 1409 (2013), but they all involved a search of a person's home or car by the government. In this case, the defendant is on the Internet, on a third party site, and is being monitored by a third-party, Facebook, not the government.

B. Facebook is Not a Government Agent.

Defendant attempts to argue that Facebook is a government agent when it is reporting illegal images to NCMEC. However, several recent cases across the county have held that internet service providers (hereafter "ISP") and electronic service providers ("hereafter ESP") are not government agents when they are reporting criminal child pornography conduct. Facebook is similar to internet service provider, AOL, who was found not to be a government

⁵ <https://variety.com/2018/digital/news/facebook-policy-updates-1202743819/>.

agent in *United States v. Stevenson*, 727 F.3d 826 (2013) and in *United States v. Keith*, 900 F.Supp.2d 33 (D.Mass. 2013).

The Eighth Circuit Court of Appeals in *Stevenson*, found that AOL, an internet service provider, was not a government agent for Fourth Amendment purposes. *United States v. Stevenson*, 727 F.3d 826 (2013). The Eighth Circuit Court reviewed the *Skinner v. Ry. Labor Executives Ass'n*, 489 U.S. 602 (1989) decision cited in defendant's motion and found that it differed from the facts in *Stevenson* because the railroad companies were required under the law to conduct the tests. Here, Title 18 U.S.C. Section 2258A(a) only requires AOL to report apparent violation of the child pornography law when they come across them. There is no requirement for the internet service provider to scan and detect child pornography. *Id.* at 829. In the *Stevenson* case, AOL, in the course of operating its' business, was using a tool called Image Detection and Filtering Process to scan files using their hash values⁶ to locate files that might be harmful to their network. *Id.* at 828. In the course of this process, it would report known files of child pornography to NCMEC when they came across it.

⁶ A hash value is “an algorithmic calculation that yields an alphanumeric value for a file.” *United States v. Stevenson*, 727 F.3d 826, 828 (8th Cir. 2013). More simply, a hash value is a string of characters obtained by processing the contents of a given computer file and assigning a sequence of numbers and letters that correspond to the file’s contents. In the words of one commentator, “[t]he concept behind hashing is quite elegant: take a large amount of data, such as a file or all the bits on a hard drive, and use a complex mathematical algorithm to generate a relatively compact numerical identifier (the hash value) unique to that data.” Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 38 (2005).

Hash values are regularly used to compare the contents of two files against each other. “If two nonidentical files are inputted into the hash program, the computer will output different results. If the two identical files are inputted, however, the hash function will generate identical output.” Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 541 (2005). Hash values have been used to fight child pornography distribution, by comparing the hash values of suspect files against a list of the hash values of known child pornography images currently in circulation. This process allows potential child pornography images to be identified rapidly, without the need to involve human investigators at every stage. *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018).

In the case of *Stevenson*, the defendant was sending a file of child pornography from his person email account on AOL to his personal Google email account when the detection system flagged it and reported it. *Id.* “In sum, the only similarity between the statutes that Stevenson cites and the *Skinner* regulations is that both include reporting obligations. A reporting requirement, standing alone, does not transform an Internet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography. *Accord United States v. Cameron*, 699 F.3d 621, 637–38 (1st Cir.2012); *United States v. Richardson*, 607 F.3d 357, 366–67 (4th Cir.2010).” *Id.* at 830. The *Stevenson* case is very similar to the case at hand. Facebook was not acting as a government agent when it located images of child pornography in the defendant’s messenger account. Facebook, as it clearly states its terms and conditions, was scanning its network on its own behalf, and does not allow child pornography. The government did not require or even ask Facebook to scan the defendant’s account. Thus, Facebook is not an agent of the government, and there was no Fourth Amendment violation on the defendant in this case.

In *United State vs. Keith*, 900 F.Supp.2d 33 (D.Mass. 2013), AOL, through a comparison of hash values, determined that a file attached to *Keith*’s email was a known image of child pornography and reported that to NCMEC. AOL systematically screened its’ users communications to prevent it from being a conduit for illicit activity. *Id* at 35. A District Court found that AOL was not a government agent⁷ after applying the factors in *United States v. Silva*, 554 F.3d 13 (1st 2009). *Id.* at 41. An email, like the one flagged by AOL in *Keith*, is very similar

⁷ The District Court in *Keith* did determine that NCMEC was a government agent, but neither the government or the defendant are in opposition to that finding. Also see the Tenth Circuit in *Unites States v. Ackerman*, 831 F.3d 1291, who determined NCMEC was a government agent.

in nature to the messages the defendant was exchanging on Facebook. AOL, like Facebook, was monitoring communications on its' platform to serve its own business interests and private interests.

Recently, the Fifth Circuit Court of Appeals in *United States v. Reddick*, held that a police detective reviewing child pornography images flagged by a private hosting service did not violate the defendant's Fourth Amendment rights. 900 F.3d 636 (2018). In that case, very similar to the one at hand, the defendant uploaded digital images to Microsoft SkyDrive, which is a cloud hosting service. SkyDrive uses a program called PhotoDNA to scan hash values of user-uploaded photographs and files to compare them against known hash values of child pornography. Once the PhotoDNA program finds a file of child pornography, a cyber-tip is created with the user's IP address, and it is sent to NCMEC. After the PhotoDNA program sent the file with Reddick's IP address to NCMEC it was forwarded to the Corpus Christi Police Department, where it was viewed by a detective. That detective then applied for a search warrant for Reddick's home and computers, which subsequently had child pornography. *Id.* at 638.

The *Reddick* Court held:

One touchstone of our Fourth Amendment jurisprudence is that the Constitution secures the right of the people against unreasonable searches and seizures conducted by the government—not searches and seizures conducted by private parties.

Under the private search doctrine, the Fourth Amendment is not implicated where the government does not conduct the search itself, but only receives and utilizes information uncovered by a search conducted by a private party.

The private search doctrine decides this case. A private company determined that the hash values of files uploaded by Mr. Reddick corresponded to the hash values of known child pornography images. The company then passed this information on to law enforcement. This qualifies as a "private search" for Fourth Amendment purposes. And the government's subsequent law enforcement actions in reviewing the images did not effect an intrusion on Mr. Reddick's privacy that he did not already experience as a result of the private search.

Id. at 637.

The Court in *Reddick* summarized “[w]hen Reddick uploaded files to SkyDrive, Microsoft’s PhotoDNA program automatically reviewed the hash values of those files and compared them against an existing database of known child pornography hash values. In other words, his “package” (that is, his set of computer files) was inspected and deemed suspicious by a private actor. Accordingly, whatever expectation of privacy Reddick might have had in the hash values of his files was frustrated by Microsoft’s private search.” *Id.* at 639. This case is similar to what Facebook did in the case at hand. Facebook, using an algorithm to flag suspicious activity, was notified the defendant had child pornography in his account. The defendant in *Reddick*, was caught by Microsoft placing child pornography images in his cloud account, he was not even sending them to another person. Here the defendant was caught sending and receiving the child pornography by Facebook and then they reported it to NCMEC. It was a private search, not a government search, and cannot be suppressed.

In conclusion, Courts have rejected the argument that individuals have a reasonable expectation of privacy when using a social media provider for illegal conduct. The social media application hosting a person’s information have a right to do a private search.

C. NCMEC’s Lawful Search and the Search Warrant.

1. NCMEC Did Not and Could Not Expand The Third Party Search.

The defendant argues at the end of his motion that NCMEC infringed on the defendant’s rights by exceeding the scope of the third party review. Doc. 117 at 19. According to the cyber-tips themselves, Facebook told NCMEC that someone at Facebook viewed the entire contents of the uploaded file sent to NCMEC. Therefore, it was impossible for NCMEC to exceed the scope of the third-party search, since Facebook reviewed everything it sent to NCMEC from the defendant’s messenger account. NCMEC did collect information on the defendant to determine

where he was located and to identify him. All of that information was collected from publicly available sources. There is no *Ackerman*, problem in this case because there was no search outside of what the private party had already done. 831 F.3d 1292 (10th Cir. 2016).

2. *The Search Warrant to Facebook Was Lawful.*

The defendant in paragraphs #63 and 64 of his motion mentions that the “warrant is overbroad.” The government assumes the defendant is discussing the Facebook warrant for the defendant’s account and answers as such. The Facebook search warrants were not overbroad and Attachment A directs Facebook to only disclose information relevant to the crime of sexual exploitation of children. Special Agent Rapp stated and set forth in paragraph #2 of the Joshi Facebook warrant, “only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Sections 2251, 2252A, 2324(a), including but not limited to the items described on Attachments A and B, which is attached hereto and incorporated herein by reference, will be found within the Facebook Account held by Ashu Joshi, where the instrumentalities, fruits and evidence of violations of Title 18, United States Code, Sections 2251, 2252A, and 2324(a) relating to material involving the sexual exploitation of minors, including but not limited to the items, as specified further in Attachments A and B, might be found.”

Attachment A stated from January 1, 2018, to the date of the warrant, that Facebook was directed to search and disclose:

- a. Any correspondence pertaining to the persuasion, inducement, and/or enticement of a **minor** to engage in **any sexual act or sexual contact**, including all opened or unopened messages;
- b. Any messages, opened or unopened, where the message or the content of the message indicates contact with individuals regarding the **sexual exploitation of children** including the production, transportation, receipt or possession of visual depictions of

minors engaged in sexually explicit conduct;

- c. Correspondence between these accounts and any other Facebook account where the content of the message discusses the **sexual exploitation of a child** including the production, transportation, receipt or possession of visual depictions of **minors** engaged in **sexually explicit conduct**, including all opened and unopened messages;
- d. Any message, opened or unopened, and any image or video file involving the **sexual exploitation of a child** including the production, transportation, receipt or possession of visual depictions of minors engaged in sexually explicit conduct which is attached to the message;
- e. Any file containing visual depictions of **minors engaged in sexually explicit conduct**;
- f. Any message, opened or unopened, and any image file that appears to contain passwords or information regarding encryption;
- g. Any and all transactional information, to include log files (transmission and usage), of all activity of the accounts which includes dates, time, method of connecting, port, dial-up, and/or location, originating Internet Protocol (IP) address and the destination IP address for all opened and unopened email, during the entire period that the account has been active, including buddy lists and terms of service violation reports;
- h. Any records of subscriber information, method of payment, or detailed billing;
- i. Copies of all the above from original storage on whatever form including printouts or digital format. The child pornography evidence should be sent by Federal Express to: **Federal Bureau of Investigation; Attn: SA David Rapp; 2222 Market Street; St. Louis, MO 63103**

Attachment A of Search Warrant 4:18MJ 7322 SPM, emphasis added.

Thus, Facebook was directed to only search and send materials that were relevant to the sexual exploitation of children or to the identification of the person who committed such crimes.

The search warrant was not overbroad and is a valid.

Lastly, the defendant alleges that the warrant should have noted that M.D. and the defendant were married. Law enforcement did not have ANY evidence that M.D. or the defendant were married on October 16, 2018, when they presented the search warrant. Both the defendant and the victim had been interviewed prior to October 16, 2018 and neither had

mentioned that they were married or had been involved in any ceremony. Further, the Facebook messages where they call each other “husband” or “wife” had not been disclosed yet by Facebook, as the warrant had not been executed. Law enforcement cannot know something that simply had not yet occurred.

Even if the Court were to find that the search warrant was written “too generally” good faith still applies. There has been absolutely no showing that any law enforcement officers in this case acted in bad faith. In this case, law enforcement officers acted in good faith relying on the search warrant to Facebook.

In *United States v. Leon*, 468 U.S. 897, 922 (1984), the Supreme Court stated: “[w]e conclude that the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion.” The Court permitted the admission of evidence from a subsequently invalidated search warrant because the officer relied in good faith on the search warrant. In *United States v. Lindsey*, 284 F.3d 874, 878 (8th Cir. 2002), the Court noted:

The good faith exception will not apply if: (1) the judge issuing the warrant was misled by statements that the affiant knew were false or would have known were false except for “his reckless disregard of the truth;” (2) “the issuing magistrate wholly abandoned his [or her] judicial role;” (3) the affidavit in support of the warrant is “so lacking in indicia or probable cause as to render official belief in its existence entirely unreasonable;” or (4) the warrant is “so facially deficient... that the executing officers cannot reasonably presume it to be valid.”

None of these issues exist in this case. Law enforcement’s reliance on the warrant was objectively reasonable because the supporting affidavit did not contain false or recklessly made statements. The supporting affidavit did not lack in indicia or probable cause sufficient to make his reliance on the affidavit unreasonable. Lastly, the warrant was not facially deficient such that law enforcement officers could have presumed it was valid. *United States v. Grant*,

490 F.3d 627, 632-33 (8th Cir. 1997). The good faith exception to the exclusionary rule can apply in this case if the Court were to determine the search warrant lacked the requisite particularity.

D. Carpenter, ECPA, and SCA Are Not Applicable in This Case.

1. *The Carpenter decision does not affect this case.*

The defendant alleges that *Carpenter* changes the outcome of the “third party doctrine.” *Carpenter v. United States*, 138 S.Ct. 2206 (2018). *Carpenter* addresses the Fourth Amendment’s application to the government’s acquisition of historical cell-site records, records which identified which cellular towers a customer’s cell phone connected with while in use. Cellular-service providers create and retain cell-site records in the ordinary course of business for their own purposes. The Supreme Court held a search warrant is required for the government to acquire historical cell-phone records revealing the location and movements of a cell-phone user. *Id.* While the defendant mentions *Carpenter* in his motion, it is never fully explained how it affects the case at hand. However, the government does not believe *Carpenter* applies to the facts of this case because Facebook data is not similar to historical cell-site data. For cell-site data, the government has to go to and through the cell phone company, a third party, to get the information. Here, Facebook has located the records during a private search and turned them over to NCMEC. The government is not requesting records or communications from anyone, like they did in *Carpenter*. When the government did request records from Facebook in this case, it served valid federal search warrants on Facebook for the records in compliance with cases like *Carpenter* and *Riley v. California*, 573 U.S. 373 (2014).

2. *There is No Violation of the Electronic Communications Privacy Act.*

The defendant alleged in his motion that Facebook's search without prior judicial authorization is in violation of the Electronic Communications Privacy Act ("ECPA"). This act is codified under Title 18 U.S.C. § 2510-22. Law enforcement in this case did not violate the ECPA because they did not intercept any contents of the defendant's electronic communications on Facebook. The communication came directly from Facebook, not the government. The government did not "intercept" any data in this case. After receiving the Facebook cyber-tip, which Facebook personnel had reviewed, the government then received a federal search warrant that was executed upon Facebook for the remaining data.

The purpose of the ECPA is to control conditions under which the interception of oral and wire communications will be permitted in order to safeguard their privacy. *Lam Lek Chong v. U.S. Drug Enforcement Admin.*, C.A.D.C.1991, 929 F.2d 729, 289 U.S.App.D.C. 136. The ECPA mandates that law enforcement shall receive a proper judicial authorization before intercepting any wire, oral or electronic communication. See 18 U.S.C. §2518. Under the ECPA, "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. 18 USC § 2510(4). The ECPA defines "contents" of electronic communications⁸ to include any information concerning the substance, purport, or meaning of that communication. Title 18 U.S.C. § 2510(8).

3. The Stored Communications Act Was Not Violated By Law Enforcement.

The Stored Communications Act (hereafter "SCA"), Title 18 U.S.C. §§2701-2712 regulates how the government can obtain customer records and actual content of

⁸ The ECPA defines "electronic communication" to mean any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce. Title 18 U.S.C. § 2510(14).

communications from telephone companies, email providers, etc. Whenever the government seeks out stored email, it must comply with the SCA, specifically §2703. In this case, the government applied for and received a search warrant for stored communications belonging to the defendant. There was no violation of the SCA because law enforcement had a valid search warrant authorizing the disclosure of the information.

D. Exceptions To The Marital Communications Privilege Applies To This Case.

The defendant contends in his motion to suppress the evidence and in this motion to dismiss the indictment that the defendant and the victim are married. The government does not believe that the defendant and the victim are lawfully married. The government will address at length in their response to the motion to dismiss the indictment, why the defendant and the victim's "marriage" is a fraud. For the purposes of responding to the defendant's argument regarding the marital privilege as laid out in the defendant's motion to suppress evidence, Doc. #117, the government is discussing why the marital privilege would not apply even if the victim and defendant were married. Again, the government is not acknowledging that they are married, because it believes the marriage is unlawful.

"The Federal Rules of Evidence state specifically that except as mandated by the Constitution or a statute, 'the privilege of a ... person ... shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience.' Fed.R.Evid. 501. *Trammel* noted the intention of Congress 'not to freeze the law of privilege' and to give the courts flexibility to make changes on a case by case basis. 445 U.S. at 47, 100 S.Ct. at 910." *United States v. Bahe*, 128 F.3d 1440, 1445 (10th Cir. 1997).

Federal courts recognize two distinct marital privileges: the marital communications privilege and the adverse spousal testimonial privilege. *United States v. Bad Wound*, 203 F. 3d 1072, 1075 (8th Cir. 2000). The adverse spousal testimony privilege prohibits compelled testimony of a witness spouse against a defendant spouse. However, that privilege may be waived and there are several expectations to it. The government is going to focus on the marital communications privilege since that is what the defendant is arguing is confidential. Doc. #117 at 11.

“The marital confidential communications privilege prohibits testimony concerning statements privately communicated between spouses during their marriage.” *United States v. Jackson*, 939 F.2d 625, 627 (8th Cir. 1991). The defendant spouse may invoke the privilege, but exceptions apply. The privilege does not apply to statements made prior to marriage, *United States v. Prensinger*, 549 F.2d 1150, 1151 (8th Cir. 1977), to those likely to be overheard by a third party, *United States v. Montgomery*, 384 F.3d 1050, 1056 (8th Cir. 1989), or when testifying spouse is a victim of a crime by the defendant spouse, *United States v. Bahe*, 128 F.3d 1440, 1445 (10th Cir. 1997). Also while there is not a lot of case law on the marital communications privilege in child abuse cases, the case law that is out there directs that the marital privilege is unavailable in cases involving child abuse. *United States v. Allery*, 526 F.2d 1362 (8th Cir. 1975).

The confines of the marital communications privilege are easy to describe. First, the privilege extends only to words or acts intended as communication to the other spouse. *Pereira v. United States*, 347 U.S. 1, 6, 74 S.Ct. 358, 361–62, 98 L.Ed. 435 (1954); *United States v. Lefkowitz*, 618 F.2d 1313, 1318 (9th Cir.), cert. denied, 449 U.S. 824, 101 S.Ct. 86, 66 L.Ed.2d 27 (1980); *Bolzer*, 556 F.2d at 951; *Lustig*, 555 F.2d at 748. Second, it covers only those communications made during a valid marriage, *see Hugle*, 754 F.2d at 865; *Lustig*, 555 F.2d at 747, unless the couple had irreconcilably separated, *see United States v. Roberson*, 859 F.2d 1376, 1381 (9th Cir.1988). Third, the privilege applies only to those marital communications which are confidential. That is, the privilege does not

extend to statements which are made before, or likely to be overheard by, third parties. *See, e.g., Pereira*, 347 U.S. at 6, 74 S.Ct. at 361–62 (statements to, or in presence of, third parties); *Lefkowitz*, 618 F.2d at 1318 (same); *United States v. McCown*, 711 F.2d 1441, 1452–53 (9th Cir.1983) (husband's request that wife write check to purchase gun at pawn shop not confidential because no indication husband intended to keep request secret from friends living in same house).” *United States v. Marashi*, 913 F.2d 724, 729-30 (9th Cir. 1990).

“The presence of a third party negatives the presumption of privacy. Wigmore, Evidence, s 2336. So too, the intention that the information conveyed be transmitted to a third person. *Id.*, s 2336. The privilege, generally, extends only to utterances, and not to acts. *Id.* s 2337. A review of Mrs. Joyce's testimony reveals that it involved primarily statements made in the presence of Brading or Miss Joyner, or both, acts of Pereira which did not amount to communications, trips taken with third parties, and her own acts.” *Pereira* at 361, 362. Statements made to a third party or that are likely to be overheard by a third party are not within the marital communications privilege. Here, Facebook clearly “overheard” their messages during a scan of their network for contraband. Facebook, is a third party conduit that sends the messages between the two parties via Facebook messenger application. The parties were not having a confidential communication in their home, or car or even over the phone. They were communicating via a third party messenger, who makes users agree to terms and conditions for us. When signing up for Facebook, a user agrees to terms and conditions, which include the right of Facebook to review user's accounts for banned activities and notifies users that Facebook reports criminal activity on their platform to the authorities.

<https://www.facebook.com/communitystandards/safety>. That is exactly what happened in this case. Facebook, the conduit for transmitting the messages, became aware they contained illegal images of child pornography, and thus, reported it to law enforcement. The defendant cannot

invoke the marital communications privilege, because those messages had been communicated to and by Facebook, a third party.

Secondly, “confidential communications involving the future or ongoing crimes in which the spouses were joint participants at the time of the communications is admissible.” *United States v. Evans*, 966 F.2d 398, 401 (8th Cir. 1992). “A widely accepted exception to the marital confidential communications privilege ‘permits witness-spouse testimony about confidential communications involving future or ongoing crimes in which the spouses were joint participants *at the time of the communications.*’ 2 *Weinstein’s Evidence* 505-36 (1991).

The rationale for the “partners in crime” exception is compelling. We protect confidential marital communications in order to “encourage the sharing of confidences between spouses.” *Id.* at 505-28. Where the communications involve the spouses’ joint criminal activity, however, the interests of justice outweigh the goal of fostering marital harmony.” *Evans* at 401. The Eighth Circuit in *Evans* goes to explain that the crime needs to be “patently illegal.” Production and Receipt of Child Pornography are patently illegal across the country. There is no marriage defense to those crimes. *United States v. Buttercase*, No. 8:12CR425, 2014 WL 7331923, at *5 (D. Neb. Dec. 19, 2014). The defendant was committing a crime when communicating with M.D. over Facebook and thus the marital communication privilege cannot be used at trial.

Further, the criminal communications between the defendant and the victim included images and videos, which are not “utterances.” “It is well settled that the communications to which the privilege applies have been limited to utterances or expressions intended by one spouse to convey a message to the other. *Pereira v. United States*, 347 U.S. 1, 6, 74 S.Ct. 358, 361, 98 L.Ed. 435, 443 (1954); 8 J. Wigmore, Evidence s 2337 (McNaughton rev. 1961). The defendant’s contention that the privilege extends to any acts done privately in the presence of

the spouse and “secured as a result of the marital relation” is not well taken.” *United States v. Smith*, 533 F.2d 1077, (8th Cir. 1976). Requesting that the victim take photos of her genitals to send to the defendant is an “act,” not a communication. The minor victim was not communicating anything to the defendant, other following his commands to produce illegal images.

In addition, another exception is when the marriage was entered into fraudulently. *United States v. Darif*, 446 F.3d 701, 706 (7th Cir. 2006), *Lutwak v. United States*, 344 U.S. 604, 614 (1953)(When good faith of marriage is pertinent and issue is whether marriage was used to scheme to defraud, privilege does not apply.) In this case, the evidence will show that the marriage was entered into fraudulently and entered into for the purpose of attempting to have a defense to these crimes. The petitions to the Court in Kentucky to validate an earlier marriage that never happened contain lies and omitted necessary elements. The “marriage” by Court Order is not valid. Under the circumstances, defendants have no marital privileges and their communications are admissible.

In conclusion, even if the Court were to find that the marriage is not a fraud, the earlier enumerated exceptions to the marital communications privilege apply and the communications can be used at trial. In particular, the communications between the defendant and the victim were on Facebook messenger, a social media application, that states clearly in its’ terms and conditions that it collects content, communications, and messages from its’ users.

<https://www.facebook.com/about/privacy/update>. The presence of a third party, in this case Facebook, negates the privilege since a third party transmitted the communication and images. The defendant and the victim were not having a private conversation in person, or even on the telephone, or even via text messages through their cell phone providers. They were utilizing a

free, publically available application that publicly discloses it monitors its' users messages and information. The interests of justice clearly outweigh the illegal communications between this couple that had not even attempted to validate their "marriage ceremony" and whom did not hold themselves out to be married. The communications on Facebook between the defendant and the victim are admissible at trial.

IV. CONCLUSION

Courts across the country have continually held that an individual does not have reasonable expectation of a privacy from a third party search on a social media application. Neither the ECPA nor the SCA applies in this case because law enforcement did not search the accounts, a third party did. Recent case law has repeatedly held, that ISPs and ESPs who report child pornography on their platforms to NCMEC are not government agents. Even if the Court were to find that the defendant and the victim are married, their illegal communications via a third party are admissible at trial and not covered by the marital privilege.

Respectfully submitted,

JEFFREY B. JENSEN
United States Attorney

s/ Colleen C. Lang

COLLEEN C. LANG, #56872MO
Assistant United States Attorney
111 South 10th Street, Room 20.333
St. Louis, MO 63102
(314) 539-2200

CERTIFICATE OF SERVICE

I hereby certify that on December 9, 2019, the foregoing was filed electronically with the Clerk of the Court to be served by email to counsel of record.

s/ Colleen C. Lang
COLLEEN C. LANG, #56872MO
Assistant United States Attorney
